PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

1. (Currently Amended) A method of generating a key stream by an apparatus comprising:

selecting at least five input words from a first array of words by a non-linear filter module, wherein each input word comprises two or more bytes;

mixing at least two words of the at least five input words to generate at least five primary mixed words by the non-linear filter module;

performing a byte-wise substitution of at least one byte of each of the five primary mixed words to generate, respectively, at least five primary intermediate words by the non-linear filter module;

mixing at least two bytes of each of the at least five primary intermediate words to generate, respectively, at least five secondary intermediate words by the non-linear filter module;

mixing at least two words of the at least five secondary intermediate words to generate at least five output words by the non-linear filter module;

selecting at least five mask words from a second array of words by a linear feedback shift register; and

combining the at least five output words with the at least five mask words to generate a key stream block for the key stream by a combining module;

wherein the first and second arrays are finite.

2. (Original) The method of claim 1, further comprising: generating the second array from the first array.

3. (Currently Amended) The method of claim 2, further comprising: using ~~a~~ the linear feedback shift register (LFSR) to generate the first array, wherein the words of the first array correspond to LFSR states.

4. (Original) The method of claim 3, further comprising: clocking the LFSR to generate the second array.

5. (Previously Presented) The method of claim 3, wherein using the LFSR to generate the first array comprises:

copying words of a key and words of an initialization vector into the LFSR;

performing a byte-wise substitution on at least one byte of a word in the LFSR to generate a corresponding replacement word in the LFSR;

mixing at least two bytes of a replacement word in the LFSR; and

mixing at least two words in the LFSR to generate the first array.

6. (Previously Presented) The method of claim 1, further comprising:

selecting updated input words from an updated first array of words for generating updated output words;

selecting updated mask words from an updated second array of words ; and

combining the updated output words with the updated mask words to generate a new key stream block for the key stream.

7. (Previously Presented) The method of claim 6, further comprising: setting the words of the first array based on first linear feedback shift register (LFSR) states; and clocking the LFSR to generate the updated first array.

8. (Previously Presented) The method of claim 6, further comprising: setting the words of the second array based on second LFSR states; and clocking the LFSR to generate the updated second array.

9. (Previously Presented) The method of claim 1, wherein the number of input words and the number of output words are equal.

10. (Previously Presented) The method of claim 1, wherein the first and second array each comprises seventeen words.

11-12. (Canceled).

13. (Previously Presented) The method of claim 1, wherein performing the byte-wise substitution of at least one byte comprises: performing a nonlinear substitution of the at least one byte.

14. (Original) The method of claim 13, wherein performing the nonlinear substitution of the at least one byte comprises: performing a key-dependent Sbox substitution on the at least one byte.

15. (Original) The method of claim 14, wherein performing the key-dependent Sbox substitution of the at least one byte comprises:

combining a first key byte with the at least one byte to generate a first combined byte; and

substituting the first combined byte with a byte value from a pre-determined array.

16. (Original) The method of claim 15, further comprising: generating the first key byte based on a secret key of one or more words.

17. (Original) The method of claim 16, wherein generating the first key comprises:

performing a byte-wise substitution of at least one byte of a word of the secret key to generate a corresponding replacement word; and

mixing at least two bytes of a replacement word to generate the first key byte.

18. (Original) The method of claim 15, wherein performing the key dependent Sbox substitution further comprises:

combining a second key byte with the substituted first combined byte to generate a second combined byte; and

substituting the second combined byte with a byte value from the predetermined array.

19. (Previously Presented) The method of claim 1, wherein mixing at least two bytes of each of the at least five primary intermediate words comprises: mixing at least two bytes using a minimum distance separable matrix multiplication.

20. (Original) The method of claim 19, wherein the minimum distance separable matrix multiplication comprises operations over a Galois Field comprising 256 elements.

21. (Canceled).

22. (Previously Presented) The method of claim 1, wherein mixing at least two of the at least five input words comprises: mixing the at least two input words based on modular arithmetic.

23. (Previously Presented) The method of claim 22, wherein mixing at least two input words comprises:

adding the input words to generate a first primary mixed word corresponding to a first input word; and

adding the first primary mixed word with a second input word to generate a second primary mixed word corresponding to the second input word.

24. (Canceled).

25. (Previously Presented) The method of claim 1, wherein mixing at least two words of the at least five secondary intermediate words comprises: mixing at least two secondary intermediate words based on modular arithmetic.

26. (Previously Presented) The method of claim 25, wherein mixing at least two of the at least five secondary intermediate words comprises:

adding the secondary intermediate words to generate a first secondary mixed word, wherein the first secondary mixed word is an output word corresponding to a first secondary intermediate word; and

adding the secondary mixed word with a second secondary intermediate word to generate an output word corresponding to the second secondary intermediate word.

27. (Currently Amended) Apparatus for generating a key stream comprising:

means for selecting at least five input words from a first array of words, wherein each input word comprises two or more bytes;

means for mixing at least two words of the at least five input words to generate at least five primary mixed words;

means for performing a byte-wise substitution of at least one byte of each of the five primary mixed words to generate, respectively, at least five primary intermediate words;

means for mixing at least two bytes of each of the at least five primary intermediate words to generate, respectively, at least five secondary intermediate words;

means for mixing at least two words of the at least five secondary intermediate words to generate at least five output words;

means for selecting at least five mask words from a second array of words; and

means for combining the at least five output words with the at least five mask words to generate a key stream block for the key stream; wherein the first and second arrays are finite.

28. (Original) The apparatus of claim 27, further comprising: means for generating the second array from the first array.

29. (Previously Presented) The apparatus of claim 27, further comprising:

means for selecting updated input words from an updated first array of words for generating updated output words;

means for selecting updated mask words from an updated second array of words; and

means for combining the updated output words with the updated mask words to generate a new key stream block for the key stream.

30. (Previously Presented) The apparatus of claim 27, wherein the number of input words and the number of output words are equal.

31-32. (Canceled).

33. (Previously Presented) The apparatus of claim 27, wherein the means for performing byte-wise substitution comprises: means for performing a key-dependent Sbox substitution on the at least one byte.

34. (Previously Presented) The apparatus of claim 27, wherein the means for mixing at least two bytes of each of the at least five primary intermediate words comprises: means for mixing at least two bytes using a minimum distance separable matrix multiplication.

35. (Previously Presented) The apparatus of claim 27, wherein the means for mixing at least two words of the at least five input words is based on modular arithmetic to generate the at least five primary mixed words.

36. (Previously Presented) The apparatus of claim 27, wherein the

means for mixing at least two words of the at least five secondary intermediate words is based on modular arithmetic to generate the output words.

37. (Currently Amended) A ~~machine-readable~~ storage medium having one or more stored instructions for generating a key stream, which when executed by a machine, causes the machine to perform operations comprising:

selecting at least five input words from a first array of words, wherein each input word comprises two or more bytes;

mixing at least two words of the at least five input words to generate at least five primary mixed words;

performing a byte-wise substitution of at least one byte of each of the five primary mixed words to generate, respectively, at least five primary intermediate words;

mixing at least two bytes of each of the at least five primary intermediate words to generate, respectively, at least five secondary intermediate words;

mixing at least two words of the at least five secondary intermediate words to generate at least five output words;

selecting at least five mask words from a second array of words; and

combining the at least five output words with the at least five mask words to generate a key stream block for the key stream;

wherein the first and second arrays are finite.

38. (Previously Presented) The medium of claim 37, further comprising one or more instructions to cause the machine to perform operations comprising: generating the second array from the first array.

39. (Canceled).

40. (Previously Presented) The medium of claim 37, wherein performing the byte-wise substitution comprises: comprises one or more instructions to cause the machine to perform operations comprising: performing a key-dependent Sbox substitution on the at least one byte.

41. (Previously Presented) The medium of claim 37, wherein mixing at least two bytes of each of the at least five primary intermediate words comprises one or more instructions to cause the machine to perform operations comprising: mixing at least two bytes using a minimum distance separable matrix multiplication.

42. (Previously Presented) The medium of claim 37, wherein mixing at least two words of the at least five input words is based on modular arithmetic to generate the at least five primary mixed words.

43. (Previously Presented) The medium of claim 37, wherein mixing at least two words of the at least five secondary intermediate words is based on modular arithmetic to generate the output words.

44. (Previously Presented) Apparatus for generating a key stream comprising:

a linear feedback shift register (LFSR) configured to generate a first array of words, wherein the words of the first array corresponds to the values of the LFSR states;

a nonlinear filter module configured to select at least five input words from the first array of words, wherein each input word comprises two or more bytes;

a first word mixing module configured to mix at least two words of the at least five input words to generate at least five primary mixed words;

a byte substitution module configured to perform byte-wise substitution of at least one byte of each of the five primary mixed words to generate, respectively, at least five primary intermediate words;

a byte mixing module configured to mix at least two bytes of each of the at least five primary intermediate words to generate, respectively, at least five secondary intermediate words;

a second word mixing module configured to mix at least two words of the at least five secondary intermediate words to generate at least five output words; and

a combining module configured to combine the at least five output words with at least five mask words selected from a second array of words to generate a key stream block for the key stream; wherein the first and second arrays are finite.

45. (Original) The apparatus of claim 44, wherein the LFSR is configured to generate the second array from the first array.

46. (Previously Presented) The apparatus of claim 44, wherein the number of input words and the number of output words are equal.

47. (Previously Presented) The apparatus of claim 44, wherein the first and second array each comprises seventeen words.

48-49. (Canceled).

50. (Previously Presented) The apparatus of claim 44, wherein the byte substitution module is configured to perform a key-dependent Sbox substitution on the at least one byte.

51. (Previously Presented) The apparatus of claim 44, wherein the byte mixing module is configured to mix at least two bytes using a minimum distance separable matrix multiplication.

52. (Previously Presented) The apparatus of claim 44, wherein the first word mixing module is further configured to mix at least two input words based on modular arithmetic to generate the at least five primary mixed words.

53. (Previously Presented) The apparatus of claim 44, wherein second word mixing module is further configured to mix at least two words of the at least five secondary intermediate words based on modular arithmetic to generate the output words.

54. (Previously Presented) The apparatus of claim 44, wherein
each output word and mask word has two or more bytes, and
the key stream block comprises five or more words, each word having two or more bytes.

55. (Previously Presented) The method of claim 1, wherein
each output word and mask word has two or more bytes, and
the key stream block comprises five or more words, each word having two or more bytes.

56. (Previously Presented) The apparatus of claim 27, wherein
each output word and mask word has two or more bytes, and
the key stream block comprises five or more words, each word having two or more bytes.

57. (Previously Presented) The medium of claim 37, wherein
each output word and mask word has two or more bytes, and
the key stream block comprises five or more words, each word having two or more bytes.